In re Patent Application of
**ROMAIN**
Serial No. **09/914,172**
Filed: **AUGUST 24, 2001**

## REMARKS

Applicant appreciates the Examiner's careful and thorough examination of the present application. By this amendment, Claims 7, 12 and 17 have been amended to features of respective dependent claims 8, 13 and 18 which have now been canceled. Claims 7, 9-12, 14-17 and 19-22 remain pending in the application. Favorable reconsideration is respectfully requested.

### I. The Invention

As described in the specification, the invention is directed to a method for avoiding a disclosure by observation of the current of protected data. The method provides security to a chaining of operations performed by an electronic circuit executing an algorithm and provides invisibility regarding analysis of electrical signals related to data transfers between various registers. More specifically, the security is provided by the presence of parasitic information which interferes with the observation, from the outside of the electronic circuit, of physical phenomena associated with the execution of useful operations.

### II. The Claims are Patentable

Claims 7-22 were rejected in view of Ugon (U.S. Patent No. 5,944,833) in view of Cohen ("Operating System Protection Through Program Evolution") or further in view of Griffin et al. (EP0448262 or corresponding document U.S. Patent No. 5,249,294) for the reasons set forth on pages 2-4 of the Office Action. As pointed out above, independent Claims

7, 12 and 17 have been amended to include the subject matter of respective dependent Claims 8, 13 and 18 which have now been canceled. Applicant contends that Claims 7, 9-12, 14-17 and 19-22 clearly define over the cited references, and in view of the following remarks, favorable reconsideration of the rejection under 35 U.S.C. §103 is requested.

Each of the independent Claims 7, 12 and 17 at least includes randomly introducing at least one dummy operation of the same type in the chaining of useful operations, and the routine maintaining a constant time interval between execution of two successive useful operations. It is these combinations of features which are not fairly taught or suggested in the cited references and which patentably define over the cited references.

The Ugon invention relates to an integrated circuit for a microprocessor controlled by at least one program and the process for using the circuit which includes means for decorrelating the running of at least one instruction sequence of a program from internal or external electrical signals of the integrated circuit. The internal or external electrical signals include timing, synchronization and status signals.

The Cohen reference is concerned with the use of program evolution as a technique for defending against automated attacks on operating systems. The Examiner pointed to the section on "Garbage Insertion" for the teaching that any sequence of instructions that are independent of the in-line sequence can be inserted into the sequence without altering the effective program execution. Each added

instruction increases both time and space, but can fool programs that look for specific instruction sequences.

The Griffin patent is concerned with determination of time of execution of a data processing routing in relation to an occurrence of a prior externally observable event. A procedure known as a "clock attack" is prevented by a method that inhibits synchronization with externally generated instructions by preventing determination of the time of execution predetermined data processing routine in relation to occurrence of an externally observable event that precedes the execution of the predetermined routine. The method includes the step of randomly varying the duration between the occurrence of the externally observable event and the execution of the predetermined routine. The method also provides a delay of a variable duration between routines.

Applicant maintains that the Examiner has misinterpreted the cited reference to Griffin. Specifically, the Examiner asserts (page 4 of the Office Action) that Griffin teaches the desirability of "providing the same duration between instructions to prevent subroutines from being distinguished from one another." Applicant notes that Griffin is concerned with the duration of the interim routines being a random variable to provide a delay of a variable duration between routines (see Col. 3 of Griffin). Indeed, there is no teaching of "maintaining a constant time interval between execution of two successive useful operations", as claimed. For this reason alone, the combination of teachings cannot result in the invention as claimed.

In re Patent Application of
**ROMAIN**
Serial No. **09/914,172**
Filed: **AUGUST 24, 2001**
/

Secondly, Applicant maintains that the Examiner is impermissibly using the teachings of Applicant's own patent application as a roadmap to modify the prior art. Again, there is no disclosure or teaching in any of the cited references of "maintaining a constant time interval between execution of two successive useful operations."

As the Examiner is aware, to establish a prima facie case of obviousness, there must be some suggestion or motivation, either in the reference itself or in the knowledge generally available to one of ordinary skill in the art, to modify the reference; and, the prior art reference must teach or suggest all the claim features. The initial burden is on the Examiner to provide some suggestion of the desirability of doing what the Applicants have done. To support the conclusion that the claimed invention is directed to obvious subject matter, either the reference must expressly or impliedly suggest the claimed invention or the Examiner must present a convincing line of reasoning as to why the artisan would have found the claimed invention to have been obvious in light of the teachings of the reference. Both the suggestion to make the claimed combination and the reasonable expectation of success must be founded in the prior art and not in Applicants' disclosure.

There is simply no teaching or suggestion in the cited reference to provide the combination of features as claimed. Accordingly, for at least the reasons given above, Applicant maintains that the cited references do not disclose or fairly suggest the invention as set forth in Claims 7, 12 and 17. Furthermore, no proper modification of the teachings

of these references could result in the invention as claimed. Thus, the rejection under 35 U.S.C. §103(a) should be withdrawn.

It is submitted that the independent claims are patentable over the prior art. In view of the patentability of the independent claims, it is submitted that their dependent claims, which recite yet further distinguishing features are also patentable over the cited references for at least the reasons set forth above. Accordingly, these dependent claims require no further discussion herein.

**III. Conclusion**

In view of the foregoing remarks, it is respectfully submitted that the present application is in condition for allowance. An early notice thereof is earnestly solicited. If, after reviewing this Response, there are any remaining informalities which need to be resolved before the application can be passed to issue, the Examiner is invited and respectfully requested to contact the undersigned by telephone in order to resolve such informalities.

Respectfully submitted,

PAUL J. DITMYER
Reg. No. 40,455
Allen, Dyer, Doppelt, Milbrath & Gilchrist, P.A.
255 S. Orange Avenue, Suite 1401
Orlando, Florida 32802
407-841-2330
Attorney for Applicant

In re Patent Application of
**ROMAIN**
Serial No. **09/914,172**
Filed: **AUGUST 24, 2001**

**CERTIFICATE OF FACSIMILE TRANSMISSION**

I HEREBY CERTIFY that the foregoing correspondence has been forwarded via facsimile number 571-273-8300 to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 this 4th day of January, 2006.